

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

- 1 1. (Currently amended) A method for sharing a secure communication
2 session, the method comprising:
3 establishing ~~the secure communication session~~ a secure socket layer (SSL)
4 session between a client and a ~~second~~ first server, wherein the first server
5 publishes on a database a set of session state information for the SSL session, and
6 wherein the SSL session state information includes:
7 an SSL session identifier;
8 a read key for encrypting communications from the client;
9 a write key for encrypting communications from the first server;
10 an encrypted running message digest; and
11 a message digest key which is used to encrypt the running message
12 digest; and
13 wherein the first server ~~secure communication session~~ is associated
14 with a session identifier, wherein the second server continually changes a ~~the~~
15 running message digest as messages are sent through the ~~secure~~
16 ~~communication~~SSL session, and wherein the ~~second~~ first server publishes updates
17 to the running message digest to a ~~the~~ database, and wherein the running message
18 digest is associated with the session identifier on the database;
19 receiving a ~~first~~ message from the client at a ~~first~~ second server, wherein
20 the ~~first~~ message includes the SSL session identifier, and wherein the client, the
21 first server, the second server, and the database are different from one another;

22 determining that an SSL session corresponding to the received session
23 identifier is not configured on the second server;
24 querying the database with the received SSL session identifier;
25 retrieving from the database identifier the SSL session state information
26 which corresponds to the received SSL session identifier and which is published
27 by the first server;~~the running message digest by the first server from the database~~
28 ~~using the session identifier; and~~
29 establishing an SSL session between the client and the second server with
30 the same SSL session identifier based on the retrieved SSL session state
31 information; and
32 using the running message digest to send a second message from the first
33 second server to the client through the ~~secure communication~~SSL session without
34 establishing a separate ~~secure communication~~SSL session between the client and
35 the ~~second~~first server.

1 2-8. (Canceled).

1 9. (Canceled).

1 10. (Previously presented) The method of claim 1, wherein retrieving the
2 running message digest includes authenticating and authorizing the first server.

1 11-12 (Canceled).

1 13. (Currently amended) A computer-readable storage medium storing
2 instructions that when executed by a computer cause the computer to perform a
3 method for sharing a secure communication session, the method comprising:

4 establishing ~~the secure communication~~ an SSL session between a client
5 and a ~~second~~ first server, wherein the first server publishes on a database a set of
6 session state information for the SSL session, and wherein the SSL session state
7 information includes:
8 _____ an SSL session identifier;
9 _____ a read key for encrypting communications from the client;
10 _____ a write key for encrypting communications from the first server;
11 _____ an encrypted running message digest; and
12 _____ a message digest key which is used to encrypt the running message
13 _____ digest; and
14 _____ wherein the first server ~~secure communication session is associated~~
15 with a session identifier, wherein the second server continually changes a ~~the~~
16 running message digest as messages are sent through the ~~secure~~
17 ~~communication~~SSL session, and wherein the ~~second~~first server publishes updates
18 to the running message digest to a ~~the~~ database, and wherein the running message
19 digest is associated with the session identifier on the database;
20 receiving a ~~first~~ message from the client at a ~~first~~ second server, wherein
21 the ~~first~~ message includes the SSL session identifier, and wherein the client, the
22 first server, the second server, and the database are different from one another;
23 _____ determining that an SSL session corresponding to the received session
24 identifier is not configured on the second server;
25 _____ querying the database with the received SSL session identifier;
26 retrieving from the database the identifierSSL session state information
27 which corresponds to the received SSL session identifier and which is published
28 by the first server; and
29 _____ establishing an SSL session between the client and the second
30 server with the same SSL session identifier based on the retrieved SSL session

31 ~~state information; and running message digest by the first server from the database~~
32 ~~using the session identifier; and~~
33 using the running message digest to send a second message from the ~~first~~
34 ~~second~~ server to the client through the ~~secure communication~~ SSL session without
35 establishing a separate ~~secure communication~~ SSL session between the client and
36 the ~~first~~ second server.

1 14-20. (Canceled).

1 21. (Canceled).

1 22. (Previously presented) The computer-readable storage medium of
2 claim 13, wherein retrieving the running message digest includes authenticating
3 and authorizing the first server.

1 23-24 (Canceled).

1 25. (Currently amended) An apparatus that shares a secure communication
2 session, comprising:
3 an establishing mechanism configured to establish ~~the secure~~
4 ~~communication~~ an SSL session between a client and a ~~second~~ first server, wherein
5 the first server publishes on a database a set of session state information for the
6 SSL session, and wherein the SSL session state information includes:
7 an SSL session identifier;
8 a read key for encrypting communications from the client;
9 a write key for encrypting communications from the first server;
10 an encrypted running message digest; and
11 a message digest key which is used to encrypt the running message

12 digest; and
13 wherein the first server~~secure communication session is associated~~
14 ~~with a session identifier, wherein the second server continually changes a~~the
15 running message digest as messages are sent through the ~~secure~~
16 ~~communication~~SSL session, and wherein the ~~second~~first server publishes updates
17 to the running message digest to ~~a~~the database, ~~and wherein the running message~~
18 ~~digest is associated with the session identifier on the database;~~
19 a receiving mechanism configured to receive a ~~first~~ message from the
20 client at a ~~first~~second server, wherein the first message includes the SSL session
21 identifier, and wherein the client, the first server, the second server, and the
22 database are different from one another;
23 a determination mechanism configured to determine that an SSL session
24 corresponding to the received session identifier is not configured on the second
25 server;
26 a query mechanism configured to query the database with the received
27 SSL session identifier;
28 a retrieving mechanism configured to retrieve from the database identifier
29 the SSL session state information which corresponds to the received SSL session
30 identifier and which is published by the first server;~~the running message digest by~~
31 ~~the first server from the database using the session identifier; and~~
32 a second establishment mechanism configured to establish an SSL session
33 between the client and the second server with the same SSL session identifier
34 based on the retrieved SSL session state information; and
35 a sending mechanism configured to use the running message digest to
36 send a second message from the ~~first~~second server to the client through the
37 ~~secure communication~~SSL session without establishing a separate ~~secure~~
38 ~~communication~~SSL session between the client and the ~~second~~first server.

1 26-32. (Canceled)

1 33. (Previously presented) The apparatus of claim 25, wherein the
2 retrieving mechanism is configured to authenticate and authorize the first server
3 prior to retrieving the running message digest.

1 34-35 (Canceled).